Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matters of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF FIRST ORION CORP.

Jennifer Glasgow
EVP, Policy and Compliance
John Ayers
VP, Corporate Development
First Orion, Corp.
500 President Clinton Ave., Suite 215
Little Rock, AR 72201

Patricia Paoletta
Adrienne E. Fowler
Harris, Wiltshire & Grannis LLP
1919 M Street, N.W., 8th Floor
Washington, DC 20036
(202) 730-1300

July 24, 2019

TABLE OF CONTENTS

INTRODUCTION 1

I. The Commission should encourage widespread adoption of SHAKEN/STIR while acknowledging its shortcomings. 2

A. Authentication results will be unreliable in the near term. 3

B. Authentication results will be more reliable in the long term, but still will not serve as a good proxy for the legality or illegality of calls. 4

i. An authentication failure does not reliably indicate illegality. 5

ii. Many illegal calls will not fail authentication. 6

C. The Commission should not encourage or require providers to block or label calls differently based solely on SHAKEN/STIR authentication results. 7

II. The Commission should encourage providers to use SHAKEN/STIR authentication results as one part of a holistic program to identify illegal calls. 9

A. What a holistic program would entail. 10

B. Holistic programs to identify illegal calls present a better policy solution. 11

C. Adoption of a broad safe harbor would encourage providers to implement holistic programs to accurately identify illegal calls. 13

D. The Commission should not create a single mechanism to measure the effectiveness of various holistic programs. 14

CONCLUSION 15

INTRODUCTION

As an industry leader in protecting consumers from unwanted and illegal calls for over a decade, First Orion Corp. supports the Commission's goal of stopping the deluge of illegal calls that American consumers receive daily. Commission efforts to encourage industry-wide deployment of the SHAKEN/STIR framework are an important step toward reaching that goal. The Commission, however, should avoid placing weight on SHAKEN/STIR authentication results that the framework alone cannot bear. In particular, failed authentication under SHAKEN/STIR serves as "a good proxy for illegal calls"[1] only when that information is combined with additional data. Accordingly, the Commission should also reiterate the important role analytics play in accurately identifying illegal calls, and be careful to avoid incentivizing voice providers to make call completion or call labeling decisions based *solely* on SHAKEN/STIR authentication results.

To encourage providers to aggressively leverage the call blocking authority adopted in the Declaratory Ruling and to deploy SHAKEN/STIR in the process, the Commission should give providers broad protection from legal liability associated with labeling and blocking calls that they identify as highly likely to be illegal, as long as the provider implements a holistic program to identify and respond to such calls. Such holistic programs would allow providers to identify and respond to calls that are highly likely to be illegal, while also guarding against impacting legitimate calls, including emergency communications—to the benefit of consumers, providers, and call originators alike. To qualify for legal protection from liability for erroneously identifying and treating a call as illegal, the Commission should require providers' holistic programs to include:

---

[1] *Advanced Methods to Target & Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC No. 19-51, CG Docket No. 17-59, WC Docket No. 17-97 ¶ 52 (rel. June 7, 2019) (hereinafter "FNPRM").

- Deployment of SHAKEN/STIR;
- The use of reasonable analytics (including among other factors discussed below, information provided by critical call lists);
- The ability to quickly and effectively correct erroneous call treatment; and
- Reporting on the number of consumers protected and the number of calls treated.

As the NANC Call Authentication Trust Anchor Working Group noted, a safe harbor from "unintended blocking" or mislabeling based on a program where "analytics are overlaid on the [SHAKEN/STIR] framework . . . would provide a strong incentive for communications service provider adoption of SHAKEN . . . . Such liability protection may override reluctance to participate in SHAKEN, *particularly in its early stages*."[2] First Orion agrees that a broad safe harbor is necessary to encourage aggressive unwanted call blocking actions to protect consumers.

I. The Commission should encourage widespread adoption of SHAKEN/STIR while acknowledging its shortcomings.

First Orion shares the Commission's goal of expeditious, industry-wide deployment of the SHAKEN/STIR framework. First Orion has developed in-network solutions that allow a provider to sign calls originating from its network, and to authenticate calls coming in from another network. In particular, First Orion partnered with T-Mobile to deploy the SHAKEN/STIR framework inside the mobile carrier's network, a first among major U.S. carriers.[3] Based on this experience, First Orion is confident that the SHAKEN/STIR framework can meaningfully reduce the number of illegal calls Americans receive, *but only* (1) after the framework has been broadly

---

[2] *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR*, NANC Call Authentication Trust Anchor Working Group, 19 (Apr. 18, 2019), http://nanc-chair.org/docs/mtg_docs/Apr18_CATA_WG_Report_Final.docx ("April NANC Report"). Notably, comparable language is included in the TRACED Act, which would direct the FCC to promulgate rules "establishing a safe harbor for a provider of voice service from liability for unintended or inadvertent blocking of calls or for the unintended or inadvertent misidentification of the level of trust for individual calls based, *in whole or in part*, on information provided by [the SHAKEN/STIR authentication framework]." TRACED Act, S.B. 151, 116th Congress § 3(c) (2019) (emphasis added).

[3] *T-Mobile Has Blocked Over A Billion Scam Calls, And Now Industry-Leading Tech Keeps Customers Even Safer,* First Orion (Nov. 8, 2018), https://firstorion.com/t-mobile-has-blocked-over-a-billion-scam-calls-and-now-industry-leading-tech-keeps-customers-even-safer/.

deployed and allowed to mature and (2) when providers use authentication results in conjunction with other analytical tools. As a result, the Commission should not encourage or require providers to block or label calls based on SHAKEN/STIR authentication results alone, particularly before industry broadly deploys the SHAKEN/STIR framework.

A. Authentication results will be unreliable in the near term.

As Commission staff and the North American Numbering Council have both noted, providers cannot use SHAKEN/STIR to "effectively and reliably authenticate calls" unless and until most voice providers implement the framework.[4] Many providers have not yet implemented the technical capability to generate, transmit, accept, and process the SIP-based Identity header that forms the foundation of the framework.[5] As the Commission notes, many voice service providers still operate on legacy networks, and will need to transition to complete IP-based networks for SHAKEN/STIR in its current form to work.[6] Questions also remain about how various governance authority and standards bodies will shape SHAKEN/STIR deployment.[7] Although providers should work diligently toward deploying SHAKEN/STIR, the Commission and members of the public should expect industry-wide deployment to take some time before voice providers achieve the desired level of authentication.

In First Orion's experience, implementing SHAKEN/STIR across a network can be a relatively complicated process. Due to differences among networks, each provider that deploys the framework will need to conduct successive rounds of time-intensive tests and adjustments

---

4 *See* April NANC Report, *supra* note 2, at 16 (describing the necessity of ongoing communication between governance bodies and standards-setting organizations).

5 FNPRM ¶ 55.

6 *Id*. ¶ 56.

7 *See generally Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR*, NANC Call Authentication Trust Anchor Working Group, 15 (May 18, 2018), http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf.

before deployment. Providers may also need to make further network changes as the governance authorities charged with overseeing and implementing an industry-wide certificate management process take shape, engage in technical decision-making, and react to vulnerabilities discovered and exploited by bad actors.[8] Implementing changes will require further testing, and more time.

Even after a critical mass of providers implement SHAKEN/STIR, the system, as a whole, will likely experience authentication failures unrelated to whether a call has been improperly spoofed for quite some time. For example, providers have a limited amount of time between initiating a public certificate download and completing verification of the Identity header, both of which are necessary steps to authenticating a call. Currently, this time limit results in failed authentication if the public certificate takes longer than usual to download, a scenario that happens with some frequency, particularly immediately after a provider begins signing calls with a new private key. First Orion also encounters verification failures that, upon further investigation, are due to interoperability issues between providers, software bugs, problems with certificate format, certificate repository outages or inaccessibility, or information having been uploaded improperly to the certificate repository. Realistically, these and other kinks are likely to persist for many months, if not a few years, after industry-wide deployment.

B. Authentication results will be more reliable in the long term, but still will not serve as a good proxy for the legality or illegality of calls.

Even after U.S. industry broadly implements SHAKEN/STIR and kinks are addressed system-wide, an authentication result *alone* will not give providers all the information they need to reliably tell whether any particular call is legal or illegal. An authentication result is designed to give providers information about origins of calls, the identity of callers, and the rights of the

[8] *See generally id*. at 6 (describing the necessity of ongoing communication between governance bodies and standards-setting organizations).

caller to use the number associated with the call. An authentication result does not, however, provide information about "the intent of the caller," i.e., whether the caller is "malicious or not."[9] Accordingly, the Commission should not encourage providers to block or label calls based solely or primarily on SHAKEN/STIR authentication results.

i. An authentication failure does not reliably indicate illegality.

Take the Commission's archetypal example of a call that is highly likely to be illegal: a caller has maliciously altered or inserted Identity header information, in an effort to gain full attestation or simply avoid failed authentication.[10] First Orion agrees with the Commission that in this scenario, the call is highly likely to be illegal, and providers should be able to block it without fearing an FCC enforcement action. The current SHAKEN/STIR standards, however, do not include any mechanism that would enable providers to identify whether a call originator has tampered with a header.

By way of background, if an originating carrier provides a degree of attestation for the call, the primary authentication result is simply an attestation value of A, B, or C, or an indication that the call is unverified.[11] None of these values inherently provides any information on whether a header has been maliciously altered. Instead, a terminating provider would need to conduct its own, independent data analytics on header information to determine whether the header had been altered and, if so, whether the alteration resulted from malfeasance or technical error.[12] Standing alone, the SHAKEN/STIR framework does not require providers to build in the capacity to conduct

---

9 ATIS, *Shaken 101: Mitigating Illegal Robocalling and Caller ID Scams* 5 (Jan. 2019).

10 FNPRM ¶ 52.

11 *Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN):RFC 8588*, IETF ¶¶ 4, 5 (last updated May, 14, 2019), https://datatracker.ietf.org/doc/rfc8588 ("RFC 8588").

12 *See id*.

such analytics. Instead, the framework treats data analytics, or "call verification treatment (CVT)" as an optional offering that "may be added to the architecture over time."[13] Nothing within the SHAKEN/STIR technical standards requires providers to employ CVT, much less specifies that CVT should include the capability to analyze headers for malicious alteration.[14]

Importantly, even after deployment of SHAKEN/STIR is mature within the United States, a failed authentication result could be caused by any number of factors. For example, the voice communications infrastructure will continue to have non-SIP-based network components for the foreseeable future, and currently, there is no reliable way to ensure that SHAKEN/STIR headers transit any non-SIP network involved in transmitting a communication. Additionally, because downstream providers can only identify the provider that owns the calling number, and not the provider who actually originates the call, calls placed while a customer is roaming will likely continue to fail authentication with some frequency. And widespread adoption in the United States will not necessarily result in widespread global adoption of SHAKEN/STIR, so international calls will continue to fail authentication at high rates for the foreseeable future.

ii. Many illegal calls will not fail authentication.

Using a failed authentication result as a proxy for "illegal call" would be under-inclusive (i.e., result in many or most illegal calls to continue to ring through to an end user) as well as over-inclusive (i.e., result in legal calls being misidentified as illegal in an unnecessarily large number

---

[13] Martin Dolly, *An Introduction and Overview of the SHAKEN/STIR Framework*, AT&T (Dec. 4, 2018), https://www.sipforum.org/download/an-introduction-and-overview-of-the-stir-shaken-framework/?wpdmdl=3530&refresh=5d2f083c172481563363388.

[14] IETF has proposed, but not adopted, a protocol that would require providers who implement STIR to transmit a "div" header, which would indicate that a call has been re-directed away from its original destination. *PASSporT Extension for Diverted Calls: Proposed Standard*, IETF (last updated July 12, 2019), https://datatracker.ietf.org/doc/draft-ietf-stir-passport-divert/. A div header value would not differentiate between calls that are legitimately diverted to a new destination (such as call forwarding services) and calls that are maliciously diverted to a new destination (by manipulating header information or otherwise).

of instances). Assume for a moment that SHAKEN/STIR could perfectly identify improperly spoofed calls. Even in this scenario, some fully authenticated calls would be illegal. After all, criminals can place calls without illegally spoofing numbers, particularly when a fraudster can switch providers any time cancellation of service occurs or seems imminent. SHAKEN/STIR would allow full authentication of these calls, and providers could not use SHAKEN/STIR to identify such calls as illegal and block or label the calls in real time.[15]

Scammers are also likely to find ways to engage in illicit spoofing while still achieving full or partial attestation. For example, scammers may increasingly focus on hacking into private branch exchange ("PBX") systems belonging to legitimate organizations. Calls flowing through such a hacked system could easily receive full authentication. Furthermore, illegal callers are likely to develop other approaches to have their calls fully authenticated in the future.[16] Providers will only catch these calls, and help prevent them from causing public harm, if they do more than simply deploy the SHAKEN/STIR standards as currently written.

C. The Commission should not encourage or require providers to block or label calls differently based solely on SHAKEN/STIR authentication results.

As discussed above, SHAKEN/STIR is unlikely to reliably and consistently authenticate calls in the near-term. And even when SHAKEN/STIR authentication results can more reliably authenticate a call originator's identity, whether a caller's identity is verified or unverified does

---

[15] *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR*, NANC Call Authentication Trust Anchor Working Group, 6 (May 18, 2018), http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf. As discussed in further detail below, SHAKEN/STIR might help the FCC, the Federal Trade Commission, and state attorneys general to identify and bring an enforcement action against the operation after-the-fact. *See generally* RFC 8588 (discussing forensic use of the "origid" value).

[16] *See generally Scam Call Trends and Projections Report (Fall 2018)*, First Orion (2018) https://ecfsapi.fcc.gov/file/109272058817712/FirstOrion_Scam_Trends_Report_FINAL%20(002)%20(002).pdf (describing scammers' uncanny ability to shift tactics in response to industry solutions).

not serve as a proxy for whether a call is legal or illegal. Accordingly, the Commission should not encourage or require providers to take any action based solely on authentication status. For example, because authentication value is not a proxy for legality, creating a safe harbor from Commission enforcement actions "for providers that choose to block calls (or a subset of calls) that fail . . . authentication under the SHAKEN/STIR framework"[17] would provide very limited relief to members of the public who receive a deluge of unlawful calls and may fall prey to increasingly sophisticated scams.[18] Providers are likely to gain little market advantage by blocking calls that fail authentication when doing so results in over- and under-blocking of illegal calls. Thus, such a safe harbor also might not appropriately incentivize providers to speed up their deployment of SHAKEN/STIR.

Similarly, providers should not be required or encouraged to display information to consumers about "whether a call has been authenticated"[19] when authentication is not a reliable predictor of whether a call is illegal or unwanted. First Orion has long worked to empower and educate members of the public, so that they can play their own part in protecting themselves from illegal calls. Currently, approximately 23% of U.S. mobile customers receive an on-screen "Scam Likely" notification when First Orion determines that a call is highly likely to be illegal. These labels have a powerful effect. Call answer rates for individuals who receive call labeling services are very low for calls identified as "Scam Likely" and higher for calls not so labeled. This high degree of consumer reliance on call labels provides a public benefit because labeling answers a question that is directly relevant to call recipients, with a high degree of accuracy: Is the person on the other end of this call likely to be a scammer?

---

17 FNPRM ¶ 51.

18 *See Scam Call Trends and Projections Report: Summer 2019*, First Orion (2019).

19 FNPRM ¶ 77.

In contrast, SHAKEN/STIR authentication results do not reliably correlate to illegal calls or any other metric that is directly relevant to call recipients. As a result, displaying SHAKEN/STIR authentication results to consumers would lessen their role. First Orion's experience suggests that many end users will heavily rely on a label showing authentication results, when the Commission, industry, and consumer advocates are fully aware that authentication results are not a reliable indicator of illegal calls. Misplaced consumer reliance on SHAKEN/STIR will result in an unacceptably high level of missed legal calls on the one hand, and consumers being more trusting toward scammers whose calls display any indicia of authentication, on the other.

The Commission also should not encourage providers to block calls from their competitors who fail to deploy SHAKEN/STIR[20] or who fail to keep certificates up-to-date.[21] While these proposals would provide a powerful incentive for providers to deploy SHAKEN/STIR and keep certificates up-to-date, their implementation would risk significant disruptions in cross-network communications. As discussed in Section II below, the Commission has less disruptive, equally effective ways to encourage expeditious deployment of SHAKEN/STIR that it should deploy instead.

II. The Commission should encourage providers to use SHAKEN/STIR authentication results as one part of a holistic program to identify illegal calls.

The Commission should encourage providers to deploy SHAKEN/STIR *and* use SHAKEN/STIR authentication results as one of many inputs, along with call information, as part of a holistic analytic assessment of whether a call is highly likely to be illegal. The Commission

[20] *Id*. ¶ 55.

[21] *Id*. ¶ 52.

should provide protections from legal liability to carriers that deploy such a holistic program. This approach would properly incentivize providers to deploy the SHAKEN/STIR framework, better protect members of the public both before and after the framework is widely deployed, and avoid unnecessary disruptions in the U.S. communications system.

A. What a holistic program would entail.

First Orion posits that providers will best protect their customers and other members of the public from illegal calls if they deploy a holistic program to identify illegal calls. Such a program would necessarily involve full deployment of SHAKEN/STIR capabilities on the provider's network, but it would not look exclusively or primarily at factors related to SHAKEN/STIR when evaluating whether a call is highly likely to be illegal. Instead, a provider deploying a holistic program would balance a wide variety of factors when analyzing each call, including SHAKEN/STIR authentication results and a combination of other reasonable analytical techniques, such as the techniques discussed in the Declaratory Ruling accompanying the FNPRM,[22] interrogation and analysis of call signaling data, machine learning, and other similar techniques. Additionally, while an individual provider would have flexibility in how to balance each of these inputs, a holistic program would never involve using a call identification program to disadvantage any competitor or to circumvent the Commission's rural call completion rules.

To facilitate error and complaint reporting, any holistic program should also publish and publicize how errors can be reported and how complaints can be filed. A provider should fix

[22] The Declaratory Ruling explains that providers may be able to reliably and reasonably identify illegal calls by evaluating "a combination of factors, such as: large bursts of calls in a short timeframe; low average call duration; low call completion ratios; invalid numbers placing a large volume of calls; common Caller ID Name (CNAM) values across voice service providers; a large volume of complaints related to a suspect line; sequential dialing patterns; neighbor spoofing patterns; patterns that indicate TCPA or other contract violations; correlation of network data with data from regulators, consumers, and other carriers; and comparison of dialed numbers to the National Do Not Call Registry." *See* FNPRM ¶ 35.

verified errors in a timely manner after verifying the existence of an error. However, a holistic program to identify and address illegal calls should not notify the caller in real time that they have been blocked. As First Orion has commented before to the Commission,[23] such a notification would serve primarily to alert illegal callers that they should switch tactics in order to evade detection.

Regarding critical call lists, as the Commission notes, effective analytics should take special precautions to avoid interfering with communications involving emergency response providers, while also taking great care to mitigate the risk that illegal callers will inappropriately exploit these special protections. [24] Thus, any holistic program to identify and respond to illegal calls should involve (1) checking a limited-access, centralized, industry-wide critical call list before blocking suspected illegal calls and (2) maintaining a provider-specific critical call list. However, a provider that deploys a holistic program should also not be required to "white list" numbers on either critical call list in all circumstances. For example, if a provider's program reasonably determines that the PBX associated with a local sheriff's office has been taken over by hackers, the provider should not be required to complete calls associated with the hacking incident.

B. Holistic programs to identify illegal calls present a better policy solution.

First Orion's experience demonstrates how a truly holistic program can more accurately identify illegal calls by looking to a wide variety of factors, some of which rely on SHAKEN/STIR and some of which are independent of the SHAKEN/STIR framework. For example, First Orion has developed highly accurate call identification solutions by leveraging an ever-growing number of factors, including machine-learning. It looks to patterns of anomalous calling behavior,

---

[23] *See, e.g.*, Comments of First Orion, CG Docket No. 17-59 (filed Sept. 24, 2018).

[24] FNPRM ¶¶ 63–70.

signatures of deceptive call spoofing, and, particularly when deployed within a provider's network, a technical analysis of call signaling and routing information. First Orion's advanced analytics solutions and extensive database of intelligence about calling parties enables it to adapt its models for natural disasters and other emergency scenarios, so that First Orion can appropriately attribute call pattern abnormalities to the emergency rather than inadvertently attributing such abnormalities to a scammer in error. First Orion will continue to enhance its solutions through artificial intelligence. First Orion also provides legitimate call originators with an effective and easy-to-use mechanism to register their numbers,[25] and allows both consumers and call originators to report calls that they believe should not be treated as illegal.

End users who have the ability to block calls that First Orion identifies as highly likely to be illegal (i.e., end users of First Orion apps and voice services offered by providers who deploy First Orion solutions in-network) are doing so in growing numbers, demonstrating consumer confidence in the accuracy of First Orion's holistic call identification program and a strong consumer desire to avoid illegal calls.

Meanwhile, because adopting a holistic program would require providers to implement the SHAKEN/STIR framework, the public, the Commission, and industry would be able to reap the unique benefits of broad framework deployment. In particular, broad deployment will better enable the Commission and other law enforcement bodies to identify the sources of illegal calls and to bring appropriate enforcement action against those callers.

[25] *See Improve Your Calling Experience*, Call Transparency (2019), https://www.calltransparency.com/.

C. Adoption of a broad safe harbor would encourage providers to implement holistic programs to accurately identify illegal calls.

First Orion applauds the Commission's efforts to date to reduce illegal calls, which have set the table for broad consumer protection. For example, encouraging the industry, as a whole, to expeditiously deploy SHAKEN/STIR can improve law enforcement bodies' ability to pursue scammers, and provide an additional data point for analyzing whether a call is illegal. Similarly, in its Declaratory Ruling, the Commission recognized that requiring consumers to opt into calling protection will not restore consumers' trust in telephone callers or protect them from illegal calls, and allowed call blocking based on reasonable analytics on an opt-out basis.

These efforts will all be for naught, however, if providers lack sufficient incentives to deploy SHAKEN/STIR as a part of a holistic program to identify and respond to illegal calls. A robust safe harbor is needed to provide such an incentive. As other participants in this proceeding have noted: "The record is clear that a broad safe harbor is necessary to encourage aggressive unwanted call blocking actions to protect consumers, protect service providers from liability for inadvertently blocking legal calls, and give industry the flexibility and incentives to continuously innovate."[26]

The very narrow safe harbor proposed in the FNPRM is problematic. It will not incentivize providers to actually deploy SHAKEN/STIR. Although the proposed safe harbor would protect providers from liability under the Commission's rules, providers may fear other forms of liability for erroneous call blocking. Moreover, many will likely fear consumer outcry for the over-blocking and under-blocking that would occur, if carriers block solely based on SHAKEN/STIR.

[26] Letter from Matthew Gerst, CTIA, and Farhan Chughtai, USTelecom, to Marlene H. Dortch, FCC, CG Docket No. 17-59; WC Docket No. 17-97 (filed May 30, 2019).

More importantly, the proposed safe harbor will not adequately protect consumers from illegal calls.

Instead, the Commission should adopt a safe harbor that encourages providers to adopt effective holistic programs that combine SHAKEN/STIR and reasonable analytics to identify and respond to illegal and unwanted calls. The Commission could best balance competing public policy interests by granting a safe harbor to providers that use a holistic program meeting the requirements discussed above as a means to identify calls that are highly likely to be illegal. A safe harbor from Commission enforcement actions would incentivize providers to quickly deploy SHAKEN/STIR as part of a holistic program to identify and respond to illegal calls. The Commission could make such an incentive even stronger still by expressly preempting state laws to the extent they thwart the Commission's interest in promoting responsible blocking and labeling of calls that a provider reasonably determines are highly likely to be illegal, or by clarifying that Commission or Congressional action in this space already precludes any application of state law.[27]

D. The Commission should not create a single mechanism to measure the effectiveness of various holistic programs.

By their very nature, holistic programs grant flexibility to providers. As such, it will be difficult for the Commission to create a single mechanism to measure the effectiveness of the various solutions providers use in order to identify and respond to illegal calls. Instead, to the extent the Commission examines whether a provider's program is effective, it should engage in a qualitative analysis. As part of any effort to measure efficacy, First Orion urges the Commission

[27] *Cf. Rules and Policies Regarding Calling Number Identification Service – Caller ID*, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd. 1764 (1994) ("[L]imited preemption of state regulations is necessary in some instances to ensure that our goal of facilitating the development of interstate calling party number based services is not frustrated by inconsistent state law, and that state decisions with respect to caller ID or other calling party number based services do not infringe upon the privacy interests of parties in other states.").

to avoid over-emphasizing false positives (i.e., legitimate calls that a provider erroneously identified as illegal) and under-estimating false negatives (i.e., illegal calls that a provider fails to identify as such). We do suggest, however, that as part of any safe harbor enjoyed by a provider that has deployed a holistic solution, the provider should be required to report on the number of subscribers protected by the solution, as well as the number of calls treated (blocked, labeled, or otherwise treated differently) by the solution.

CONCLUSION

The SHAKEN/STIR framework will be effective for identifying illegal calls when combined with other tools. When used alone, however, SHAKEN/STIR authentication results will be nowhere near a reliable indicator of illegality—both now and in the foreseeable future. Accordingly, the Commission should (1) adopt a robust safe harbor to encourage providers to deploy the SHAKEN/STIR framework as part of a holistic program, based on SHAKEN/STIR results and reasonable analytics (including intelligence from critical call lists), to identify and block or label calls that are highly likely to be illegal and (2) avoid inappropriately relying on quantitative efficacy metrics that will not be comparable across providers.

July 24, 2019

Respectfully submitted,

/s/ John Ayers

Jennifer Glasgow
EVP, Policy and Compliance
John Ayers
VP, Corporate Development
First Orion, Corp.
500 President Clinton Ave.
Suite 215
Little Rock, AR 72201

Tricia Paoletta
Adrienne E. Fowler
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, N.W.
8th Floor
Washington, DC 20036
(202) 730-1300